ARGUMENTS DIRECTED TO CONFEREES

In its present rejection, the Office takes the position that, while a disclosure of all limitations of Applicant's claims does not appear in any single reference, individual pieces or aspects of Applicant's claimed inventions do appear in *Zhao*, *Van Oorschot* and *Williams*, such that through the magic of *KSR*, a combined and operative whole would have been obvious to persons of ordinary skill in the art at least as of 2 December 2003 (the effective filing date of the present application). Leaving aside (for purposes of the pre-Appeal Brief conference) the propriety of the proposed combination, the Office's obviousness rejection is fundamentally premised on the specific disclosure that it attributes to *Zhao*, to *Van Oorschot* and to *Williams*. Because the disclosure that the Office attributes to these references is so clearly inconsistent with the actual contents thereof, rejections made by the Office **necessarily omit elements that would be essential to a *prima facie* case** of obviousness.

Office interpretations of the applied references, particularly of *Zhao* and *Van Oorschot*, are simply not supported by the actual disclosure thereof. At best, *Zhao* discloses a delta CRL technique without use of any hash, let alone a hash over the specific items recited by Applicant in its claims; *Van Oorschot* uses the terms "delta CRL" and "hash" in the same document, though not in any way remotely pertinent to Applicant's claims; and *Williams* discloses comparison of a received, sending-side hash over transmitted message data with a receive-side hash computed over message data received.

No reasonable interpretation of *Zhao*, *Van Oorschot* and/or *Williams* discloses or suggests, whether the references are taken alone or in combination, a delta CRL mechanism as recited in various of the claims wherein a **hash over resultant state** (e.g., a state CRL(t+1) that results after application of a particular delta CRL to an appropriate base state CRL(t)) is received transmitted, encoded or used in association with the particular delta CRL, such as to validate update to the resultant state. Accordingly, the Office has not made out a *prima facie* case of obviousness and the rejections must be withdrawn.

Clear Errors

The Office's rejection is premised on the following interpretations/assertions as to content of the applied art:

- *Zhao*: According to the Office, *Zhao* discloses "`receiving a delta coded update to a certificate revocation list (a delta CRL) together with an associated first hash value`...." *See* Office action, p. 6 (emphasis added). According to the Office, *Zhao* does not specifically disclose that "`the first hash value [is] computed as a function of at least a resultant state CRL(t+1) computable by applying the delta CRL to the CRL(t) state, and a second hash value as a function of at least the resultant local CRL state and comparing the second and first hash values`," but *Van Oorschot* does.

  With respect, even a cursory review of *Zhao* reveals that no hash value is associated with any delta CRL. For at least this reason, the Office has failed to make a *prima facie* case.

- *Van Oorschot*: As best understood by the undersigned, the Office takes the position that because *Van Oorschot* discusses delta CRLs (in col. 4) and discloses (in col. 5) of a one-way hash for improving storage efficiency of an address_list coding within a digital certificate, Applicant's claim limitations ("`the first hash value computed as a function of at least a resultant state CRL(t+1) computable by applying the delta CRL to the CRL(t) state`") are satisfied.

  Van Oorschot describes use of a hash to code a list of addresses in a digital certificate. Notwithstanding the Office's bold assertion, *Van Oorschot* does not disclose a hash over resultant state CRL(t+1) computable by applying a delta CRL to a CRL(t) state. Rather, *Van Oorschot*'s hash is over a list of addresses (e.g., network addresses, filenames, database entry identifiers or the like) encoded in a digital certificate that allows a cryptographic system to backtrack to a particular CRL that contains a CRL segment that codes a reason for revocation of the digital certificate.

With respect, about all that can be said of *Van Oorschot* (insofar as pertinence to Applicant's claims is concerned) is that the reference uses terms "delta CRL" and "hash" in the same document. Again, the Office has failed to make a *prima facie* case.

- *Williams* discloses (at p. 3) sending a message that includes encrypted message data and a digital signature that itself includes an encrypted hash value of the message data encrypted and later discloses (at p. 7) comparison of a received, sending-side hash value with a receive-side hash value computed over the message data received.

  In fairness, Williams is a perfectly reasonable reference for use of a comparison of (i) a transmit-side hash over message data transmitted with (ii) a receive-side hash over message data received to assure integrity of the message data. However, Applicant's claims recite use of a hash function computed as a function of at least some data (e.g., a resultant state) that is not the data transmitted (or received). Because neither *Williams*, nor any other applied reference discloses this claimed aspect, the Office simply **fails to make a *prima facie* case.**

Specific Claim Language

Accordingly, no reasonable interpretation of *Zhao*, *Van Oorschot* and/or *Williams* discloses or suggests, whether the references are taken alone or in combination, a method (as in independent **claim 3**):

> … for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, the method comprising:
>
> receiving a delta coded update to a certificate revocation list (a delta CRL) **together with an associated first hash value, the delta CRL encoding an update to a preceding certificate revocation list state CRL(t) and the first hash value computed as a function of at least a resultant state CRL(t+1) computable by applying the delta CRL to the CRL(t) state;**
>
> computing an update to a local certificate revocation list state by applying the received delta CRL to produce a resultant local CRL state; and
>
> validating the update at least in part **by computing a second hash value as a function of at least the resultant local CRL state** and comparing the second and first hash values.

or a method (as in independent **claim 11**):

> … for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, the method comprising:
>
> preparing a first delta coded update to a certificate revocation list (a first delta CRL), the first delta CRL encoding an update sufficient to produce a subsequent certificate revocation list state CRL(t+1) from a preceding certificate revocation list state CRL(t);
>
> **computing an associated first hash value as a function of at least the CRL(t+1) state;** and
>
> **transmitting the delta CRL and the associated first hash value** in response to a request for certificate revocation list update beyond a base t.

or a system (as in independent **claim 16**) comprising:

> first and second validation authorities (VAs) communicatively coupled to propagate certificate revocation list (CRL) information;
>
> the first VA configured to prepare delta CRLs in correspondence with updates from a certificate authority (CA), each delta CRL encoding a respective update sufficient to produce a next certificate revocation list state CRL(t+1) from a preceding certificate revocation list state CRL(t), the first VA further configured to compute respective first hash values as a function of respective sequentially adjacent pairs of states CRL(t) and CRL(t+1); and
>
> the **second VA configured** to receive the delta CRLs from the first VA, to calculate based thereon updates to local certificate revocation list states by applying the received delta CRL to produce a resultant local CRL state, and **to validate each update based at least in part on comparison of respective first hash values received from the first VA with second hash values computed as a function of respective prior local CRL states and resultant local CRL states.**

Each of the foregoing independent claims is allowable. Claims 4-10, 12-15 and 17-20, which depend from respective of the foregoing independent claims are allowable for at least the same or analogous reasons.

Art Rejections—
35 U.S.C. § 103, Zhao in view of Van Oorschot

Claims 21 and 22 stand rejected under 35 U.S.C. § 103(a) as unpatentable over *Zhao* in view of *Van Oorschot*. Applicants respectfully **traverse**. Although claims 21 and 22 are of

different scope than claims 1-20 and 23 (discussed above), errant interpretations *Zhao* and *Van Oorschot* dictate withdrawal of the these rejections as well.

In particular, no reasonable interpretation of *Zhao* and/or *Van Oorschot* discloses or suggests, whether the references are taken alone or in combination, a computer readable medium (as in independent **claim 21**) encoding and comprising:

> delta coded certificate revocation list (CRL) update data that allows a receiving validation authority to generate an updated CRL by applying the delta coded CRL update to a previous CRL state;
>
> a self-validating indicator encoded in association with the delta coded CRL update, the self-validating indicator **encoding a hash computed not as a function of the delta coded CRL update itself, but rather as a function of the next certificate revocation list state CRL(t+1) which may be generating by applying the delta coded CRL update to a previous certificate revocation list state CRL(t);** and
>
> a digital signature establishing identity of a source of the computer readable encoding.

Claim 22, which depends from independent claim 21 is allowable for at least the same or analogous reasons.